

1355 U.S. PTO
09/24/99

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 1341.1030/JDH

First Named Inventor or Application Identifier:

Ryota AKIYAMA, et al.

Express Mail Label No.

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ [X] Fee Transmittal Form
2. ☒ [X] Specification, Claims & Abstract [Total Pages: 37]
3. ☒ [X] Drawing(s) (35 USC 113) [Total Sheets: 6]
4. ☒ [X] Oath or Declaration [Total Pages: 4]
 - a. ☒ [X] Newly executed (original or copy)
 - b. ☐ [] Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional with Box 17 completed)
 - i. ☐ [] **DELETION OF INVENTOR(S)**
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. ☐ [] Incorporation by Reference (usable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ [] Microfiche Computer Program (Appendix)
7. ☐ [] Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
 - a. ☐ [] Computer Readable Copy
 - b. ☐ [] Paper Copy (identical to computer copy)
 - c. ☐ [] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ [X] Assignment Papers (cover sheet & document(s))
9. ☐ [] 37 CFR 3.73(b) Statement (when there is an assignee) [] Power of Attorney
10. ☐ [] English Translation Document (if applicable)
11. ☐ [] Information Disclosure Statement (IDS)/PTO-1449[X] Copies of IDS Citations
12. ☐ [] Preliminary Amendment
13. ☒ [X] Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. ☐ [] Small Entity Statement(s) [] Statement filed in prior application, status still proper and desired.
15. ☒ [X] Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☐ [] Other:

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:☐ [] Continuation ☐ [] Divisional ☐ [] Continuation-in-part (CIP) of prior application No: / **18. CORRESPONDENCE ADDRESS**STAAS & HALSEY
Attn: James D. Halsey, Jr.
700 Eleventh Street, N.W., Suite 500
Washington, DC 20001Telephone: (202) 434-1500
Facsimile: (202) 434-1501

NEW APPLICATION FEE TRANSMITTAL

Attorney Docket No.	1341.1030/JDH
Application Number	Unassigned
Filing Date	September 24, 1999
First Named Inventor	Ryota AKIYAMA, et al.

AMOUNT ENCLOSED	\$ 1,790.00
-----------------	-------------

FEE CALCULATION (fees effective 10/01/97)

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
TOTAL CLAIMS	23	- 20 =	3	X \$ 18.00 =	\$ 54.00
INDEPENDENT CLAIMS	15	- 3 =	12	X \$ 78.00 =	936.00
MULTIPLE DEPENDENT CLAIMS (any number; if applicable)				+ \$270 00 =	0.00
BASIC FILING FEE					+ 760.00
Total of above Calculations =					\$ 1,750.00
Surcharge for late filing fee, Statement or Power of Attorney (\$130.00)					+ 0.00
Reduction by 50% for filing by small entity (37 CFR 1.9, 1.27 & 1.28).					- 0.00
TOTAL FILING FEE =					\$ 1,750.00
Surcharge for filing non-English language application (\$130.00; 37 CFR 1.52(d))					+ 0.00
Recordation of Assignment (\$40.00; 37 CFR 1.21(h)(1))					+ 40.00
TOTAL FEES DUE =					\$ 1,790.00

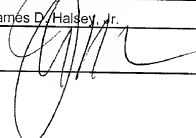
METHOD OF PAYMENT

- ☒ Check enclosed as payment.
- ☐ Charge "TOTAL FEES DUE" to the Deposit Account No., below.
- ☐ No payment is enclosed and no charges to the Deposit Account are authorized at this time.

GENERAL AUTHORIZATION

- ☒ If the above-noted "AMOUNT ENCLOSED" is not correct, the Commissioner is hereby authorized to credit any overpayment or charge any additional fees necessary to:
- | | |
|----------------------|----------------|
| Deposit Account No. | 19-3935 |
| Deposit Account Name | STAAS & HALSEY |
- ☒ The Commissioner is also authorized to credit any overpayments or charge any additional fees required under 37 CFR 1.16 (filing fees) or 37 CFR 1.17 (processing fees) during the prosecution of this application, including any related application(s) claiming benefit hereof pursuant to 35 USC § 120 (e.g., continuations/divisionals/CIPs under 37 CFR 1.53(b) and/or continuations/divisionals/CPAs under 37 CFR 1.53(b)) to maintain pendency hereof or of any such related application.

SUBMITTED BY: STAAS & HALSEY

Typed Name	James D. Halsey, Jr.	Reg. No.	22,729
Signature		Date	September 24, 1999

AUTHENTICATION SYSTEM, AUTHENTICATION METHOD,

SIGNING APPARATUS, SIGNING METHOD,

CERTIFYING APPARATUS, CERTIFYING METHOD, AND

A COMPUTER-READABLE RECORDING MEDIUM WITH A PROGRAM

5 MAKING A COMPUTER EXECUTE THE METHOD RECORDED THEREIN

FIELD OF THE INVENTION

The present invention relates to an authentication system,
an authentication method, a signing apparatus, a signing method,
10 a certifying apparatus, a certifying method, and a recording
medium for the same for creating an authenticator by applying
a one-way function to electronic data, appending a signature
to the electronic data and checking authentication of the
electronic data using the authenticator. The invention more
15 particularly relates to an authentication system, an
authentication method, a signing apparatus, a signing method,
a certifying apparatus, a certifying method, and a recording
medium for the same which can efficiently prevent forgery of
the authenticator.

BACKGROUND OF THE INVENTION

In association with recent development in the computer
technology, there has increased an opportunity to accumulate
electronic data such as a document prepared with characters,
25 numerals, and strings of symbols in a database, or to transfer

the data via a network. Considering these facts, how to avoid forgery of electronic data accumulated in a database or forgery of data during data communications has become a serious problem.

For solving the problem, there has been known an authentication technology in which an authenticator created by applying a one-way function to electronic data is appended thereto when the electronic data is transmitted and whether transmitted data is forged or not is verified using this authenticator when the electronic data is received.

More specifically, a station which transmits the electronic data (signing station) divides the electronic data into specified blocks, subjects the data to a signature processing by applying a one-way function such as a hash function to each of the divided data blocks, and transmits the data obtained through the processing to a distant station (certifying station). While a station which receives the electronic data creates an authenticator by applying a one-way function to a portion of the data other than the authenticator in the received electronic data, compares the created authenticator with the authenticator included in the electronic data, and verifies whether the electronic data has been forged or not.

However, even if the conventional technology described above is used, forgery of or tampering of electronic data can not possibly be verified if the portion of the authenticator

itself is forged, namely if the signature is forged. Therefore, prevention of forgery of the signature becomes an issue that need to be resolved.

When a hash function is used, for example, it is possible
5 to make more difficult to forgery of electronic data by making longer a processed block length of the hash function. However, it is not realistic to make the processed block length of the hash function extraordinarily long.

Especially, a conventional type of hash function is
10 formed not based on an organized structural method but based on, in many cases, an empirical or an intuitive method obtained by combining a logical operation such as AND and OR with four rule of arithmetic in a complex manner. Therefore, enormous man power is required for experiments or the like when the block
15 length of the hash function is to be increased.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide, for the purpose of solving the problem described above, an
20 authentication system, an authentication method, a signing apparatus, a signing method, a certifying apparatus, a certifying method, and a recording medium for the same which can efficiently prevent the forgery of the authenticator, when checking the authentication of the electronic data from an
25 authenticator created using a one-way function.

With the present invention, a signing station creates a plurality of authenticators using a plurality of one-way functions then and links these plurality of authenticators to the electronic data, so that the length of the authenticators
5 to be appended to the information can easily be made longer, which makes it possible to reduce a probability of misidentification of a forged authenticator.

With the present invention, the whole authenticator is not linked to the information, but only a portion of data
10 obtained by truncating each of the authenticator is linked, which makes it more difficult for a third party to forge the authenticator.

With the present invention, a one-way operation is performed with the data using a different key, so that the length
15 of the authenticators to be appended to the information can be made longer without utilizing a special one-way operation.

With the present invention, authenticators are discretely and independently prepared in parallel with each other, so that a plurality of authenticators can quickly be
20 prepared.

With the present invention, an authenticator is prepared by utilizing intermediate data generated when other the authenticator is created, so that generation of the authenticator is made more complicated, which makes it still
25 difficult for a third party to forge the authenticator.

With the present invention, a signing station executes a step of preparing a plurality of authenticators by applying a different one-way function to each data, and a step of linking the created authenticators to the information, so that the length of the authenticators to be appended to the information can easily be made longer, which makes it possible to reduce a probability of misidentification of a forged authenticator.

With the present invention, there is a step of not linking the created whole authenticators to the information but linking only a portion of the data obtained by truncating each of the authenticators, which makes it more difficult for a third party to forge the authenticators.

With the present invention, there is a step of performing a one-way operation with the data using a different key, so that the length of the authenticators to be appended to the information can be made longer without utilizing a special one-way operation.

With the present invention, there are steps of discretely and independently creating the authenticators in parallel with each other, so that a plurality of authenticators can quickly be created.

With the present invention, there is a step of preparing the authenticator by utilizing an intermediate data generated when other authenticator is created, so that creation of the authenticator is made more complicated, which makes it still

difficult for a third party to forge the authenticator.

With the present invention, the program stored in the recording medium makes a signing station execute a step of creating a plurality of authenticators by applying a different one-way function to each data, and a step of linking the created authenticators to the information, so that the length of the authenticators to be appended to the information can easily be made longer, which makes it possible to reduce a probability of misidentification of the forged authenticator.

Other objects and features of this invention will become understood from the following description with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a system configuration of the authentication system used in an embodiment of the present invention;

Fig. 2A and Fig. 2B show more specific configuration (independent and multi-parallel configuration) of the authentication system shown in Fig. 1;

Fig. 3A and Fig. 3B show a case where the authentication system shown in Fig. 1 operates independently in three parallel branches;

Fig. 4A shows configuration and Fig. 4B shows operation when the hash units 2 perform parallel processing in association with each other;

Fig. 5 is a view showing one example of a document as an object for processing; and

Fig. 6A and Fig. 6B explain the safety in the authentication system used in the embodiment.

5

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Detailed description is made hereinafter for preferred embodiments of the present invention with reference to Fig. 1 to Fig. 6. It should be noted that this embodiment explains a case in which text data included in a document is the target data and an authenticator is created by applying a hash function to this target data.

Fig. 1 is a block diagram showing system configuration of the authentication system used in the embodiment of the present invention. In the left-hand side of Fig. 1 is a signature side (a signing station) which creates an authenticator by applying a hash function to the text data and links this authenticator to the text data before transmission. In the right-hand side of Fig. 1 is an authentication side (a certifying station) which creates an authenticator by applying a hash function to the data obtained by removing the authenticator from the received data, comparing the created authenticator with the authenticator included in the received data to check the correctness of the text data. Although it is assumed in this embodiment that a communication error will

not occur in the process of transmission of data from the signing station to the certifying station. However, occurrence of error may be prevented by using an error-correction code or the like in some other cases.

5 At first, configuration of the signing station is described. As shown in Fig. 1, the signing station comprises a plurality of hash units 2 and keys 3, and a linking unit 5, and it is assumed that data 1 is input to this signing station.

10 The data 1 is text data as an object for transmission to the certifying station and consists of a plurality of data D1 to Dn obtained by dividing the data into each data with a size corresponding to a data length for a hash function. This data 1 is text data which contains numerals, characters, or symbols included in a document shown in Fig. 5, and, for example, "The
15 present invention" shown in Fig. 5 corresponds to data D1.

 The hash units 2 have one-way functions for converting the data D1 to Dn using keys K1 to Kn to authentication signs CS1 to CSn respectively, and they output the converted authentication signs CS1 to CSn to the linking unit 5. Although
20 it is assumed that the hash units 2 perform processing corresponding to a known hash function in a protocol or the like for a method of verifying authentication signs based on the conventional technology, it is not always required that reverse conversion is ensured.

25 The keys 3 are the secret keys used when the hash units

2 perform scramble of one-way data compression, and authentication signs 4 are prepared by the hash units 2 according to the keys K1 to Kn.

5 The linking unit 5 links the authenticators 4 created by the hash units 2 to data D1 to Dn that should originally be transmitted, and the linked authenticators 4 are appended, for example, to the end of the document as shown in Fig. 5.

10 Next, configuration of the certifying station is described. As shown in Fig. 1, the certifying station comprises a separating unit 7, a plurality of hash units 2 and keys 3, and a comparing unit 8, and data received from the signing station is input to the certifying station.

15 The separating unit 7 separates the data received from the signing station into data D1' to Dn' and the authentication signs 4. The data D1' to Dn' is inputted into the hash units 2, while the authenticators 4 are inputted into the comparing unit 8.

20 The comparing unit 8 compares the authentication signs separated from the received data with the authenticators created from the data D1' to Dn'. The comparing unit 8 certifies that the data is authentic when the authenticators are coincident with each other, and certifies that the data is forged one when the authenticators are not coincident.

25 As described above, the authentication system according to this embodiment is so configured that a signing station

prepares a plurality of authenticators CS1 to CSn using a plurality of hash units, so that a data length of authenticators can be made longer, which makes it difficult to forge the authenticator by a third party.

5 A sequence of processing by the signing station and the certifying station of the authentication system shown in Fig. 1 is described below.

(1) Creation of authenticators in the signature station:

10 (1-1) The hash units 2 create CS1 to CSn each as the authenticators 4 by performing the processing of a one-way function using a key for each of input data D1 to Dn respectively into which the text data has been divided.

15 (1-2) The linking unit 5 links the authenticators CS1 to CSn created by the hash units 2 to the data D1 to Dn. As a result, for example, authenticators of 8 digits each consisting of 4 bits are appended, for example, to the end of the text as shown in the document of Fig. 5.

20 As described above, authenticators are created with a different key for each of the data D1 to Dn into which the text data has been divided, which makes it extremely difficult for a third party to forge the authenticator, thus reliability of text data being enhanced.

(2) Creation of authenticators in the certifying station:

25 (2-1) The document shown in Fig. 5 prepared in the above step (1) is separated into the authenticators CS1 to Cn and data

D1' to Dn'.

(2-2) The hash units 2 create CS1' to CSn' as the authenticators 4 for the separated data D1' to Dn' respectively by using a different key.

5 (2-3) The created authenticators CS1' to CSn' are compared with the separated authenticators CS1 to CSn, and whether the authenticators are coincident with each other or not is determined. When the authenticators are coincident, then the text data is recognized as not being forged, namely as an
10 authentic one. On the other hand, when even a single authenticator is not coincident, then the text data is recognized as being a forged one.

As described above, the certifying station creates authenticators CS1' to CSn' each with a different key for each
15 of the data D1' to Dn' separated from received data, compares the created authenticators CS1' to CSn' with the authenticators CS1 to CSn which are separated from the received data, determines the text data as an authentic one when it is determined that all the authenticators are coincident with each
20 other, on the other hand, determines the text data as a forged one when even one authenticator is not coincident.

More specific configuration (independent and multi-parallel configuration) of the authentication system shown in Fig. 1 is described. Fig. 2 is a block diagram showing more
25 specific configuration (independent and multi-parallel

configuration) of the authentication system shown in Fig. 1. Herein a case is assumed in which authenticators CS1 to CSn are created concurrently as well as in parallel from each of the input data D1 to Dn by using a different key.

5 Fig. 2A shows configuration of the authentication system, and in Fig. 2A, input data D1 to Dn is data D1 to Dn into which the text data as an object for transmission is divided. The hash units 2 create the authenticators CS using the keys K. More specifically, each of the hash units 2 consists of an EOR 21,
10 a one-way function 22 such as a hash function, and a truncator 23.

The EOR 21 executes an operation of an exclusive OR, and operates herein an exclusive OR between the input data and a value obtained in the one-way function 22 in the previous time
15 (an initial value IV is used for the first time).

The one-way function (corresponds to a one-way function device) 22 creates an irreversible authenticator CS with the help of the one-way function from the data processed in the EOR 21 based on the key K.

20 The truncator 23 truncates the authenticator CS prepared by the one-way function 22 and outputs the truncated authenticator. When the authenticator created by the one-way function 22 is outputted as it is, data length of the authenticator is naturally increased. However, an increase in
25 the data length of the authenticator CS does not increase the

safety of data but it only increase the amount of data to be transmitted.

Therefore, the truncator 23 truncates a portion of the authenticator created by the one-way function 22 so that increase in a data length of the authenticator CS is made really useful. Even if the authenticator is truncated, a symbol space same as that in the case where the authenticator are transmitted without being truncated is formed, therefore, security of data is not possibly reduced. Further, the security surely increases due to the truncation, because a third party will not know where the authenticator is truncated.

Output data (D1 to Dn, CS1 to CSn) is obtained, as shown in Fig. 5, by linking the created authenticators CS1 to CSn to input data D1 to Dn.

Fig. 2B shows how the authenticator CS is generated, and a portion of the left of Fig. 2B shows especially how the authenticator CS1 is generated.

In the left portion in Fig. 2B,

① "IV = Public constant" indicates that a public constant is set as the initial value IV which is inputted into the EOR 21 forming a part of the hash unit 2 in the far left side of Fig. 2A.

② "EK1[IV(+D1)]=L11" indicates that the EOR 21 in Fig. 2A operates an exclusive OR between the initial value IV set in

① and the input data D1, and that the one-way function 22

performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L11.

③ "EK1[L11(+)D2]=L12" indicates that the EOR 21 in Fig. 2A operates an exclusive OR between the value L11 obtained in ② and the second input data D2, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L12.

④ "EK1[L1(n-1)(+)Dn]=L1n" indicates that the EOR 21 in Fig. 2A operates, similarly as described above, an exclusive OR between the previously obtained value L1 (n-1) and n-th data Dn, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L1n.

⑤ "Tr[L1n]=CS1" indicates that, when the operation is performed with respect to the last i.e. the n-th data Dn, a result of the last operation is outputted as the authenticator CS1.

Thus, the authenticator CS1 can be created by using the key 1 and initial value IV through the sequence of ① to ⑤ described above.

The central and the right portions of Fig. 2B respectively show, similarly to the sequence of ① to ⑤ in the left portion, sequence of computing the authenticators CS2 and CS3

respectively. By repeating the same operation, authenticators up to CSn can also be computed.

As described above, it is possible to concurrently compute authentication signs CS1 to CSn by using the keys K1 to Kn independently in n parallel branches. Herein, a forgery probability per CSn is $1/2^{np}$ (where p is a bit length of the authentication sign). This forgery probability can be reduced by increasing a number of authenticators CS. Even if a number of authenticators CS is increased, because the processing is done parallel, a time required for the processing does not change.

Next, a configuration as well as an operation is described when $n=3$ (independent triple-parallel configuration) in Fig. 2A and Fig. 2B with reference to Fig. 3A and Fig. 3B. Fig. 3A is a view showing a case where the authentication system shown in Fig. 1 operates independently in three parallel branches.

Fig. 3A shows configuration of a case where n in Fig. 2A is set to 3. The same reference numerals as those in Fig. 2A are assigned to the hash units 2, the EOR 21, the one-way function 22, and the truncator 23, and detailed description thereof is omitted herein.

Fig. 3B shows how the authenticators CS1 to CS3 are generated in the hash units 2. Especially, the left portion of Fig. 3B shows a sequence of processing when the authenticator CS1 is created from the input data D1 to D3, the key K1, and

initial value IV shown in Fig. 3A.

In the left portion in Fig. 3B,

①' "IV = Public constant" indicates that a public constant is set as the initial value IV which is inputted into the EOR 21 in the first hash unit 2 from the left side of Fig. 3A.

②' "EK1[IV(+)D1]=L11" indicates that the EOR 21 in Fig. 3A operates an exclusive OR between the initial value IV set in ①' and the first input data D1, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L11.

③' "EK1[L11(+)D2]=L12" indicates that the EOR 21 in Fig. 3A operates an exclusive OR between the value L11 obtained in ②' and the second input data D2, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L12.

④' "EK1[L12(+)D3]=L13" indicates that the EOR 21 in Fig. 3A operates, similarly as described above, an exclusive OR between the previously obtained value L12 and 3rd data D3, and that the one-way function 22 performs a one-way operation (e.g., an operation by a hash function) with respect to the value obtained by operating the exclusive OR using the key K1 to obtain a value L1n.

⑤' "Tr[L13]=CS1" indicates that, when the operation is

performed with respect to the last i.e. 3rd data D3, a result of the 3rd operation is outputted as the authenticator CS1.

The central portion and the right portion of Fig. 3B respectively show, similarly to the sequence of ①' to ⑤' in left portion, sequence of computing authenticators CS2 and CS3.

Through the above mentioned sequence of ①' to ⑤', it is possible to concurrently and independently compute authenticators CS1 to CS3 by using the keys K1 to K3 respectively.

A case has been explained above in which the hash units 2 perform parallel processing in three branches concurrently and independently. However, the present invention is not limited to this and it may be applied to a case in which the hash units 2 perform parallel processing in association with each other and not concurrently.

The case in which the hash units 2 perform parallel processing in association with each other is explained here. Fig. 4A shows configuration and Fig. 4B shows operation when hash units 2 perform parallel processing in association with each other. More specifically, these figures show a case in which n is set to 3 and intermediate data in a previous stage is used as an initial value in the next stage.

Fig. 4A shows configuration of a case where n is set to 3 and intermediate data in a previous stage is used as the initial value in the next stage. The same reference numerals as those

in Fig. 2A are assigned to the hash units 2, the EOR 21, the one-way function 22, and the truncator 23, and detailed description thereof is omitted herein.

This case is different from the case shown in Fig. 3A in that the initial value IV is set according to the intermediate data generated in other hash unit 2. The hash units 2 are so configured that as the initial value IV, intermediate data generated in other hash unit 2 is substituted. This configuration allows the authenticator CS to become more complicated, therefore, security is highly enhanced.

Fig. 4B shows how the authenticators CS1 to CS3 are generated in the hash units 2. Especially, the left portion of this figure shows a sequence of computing the authenticator CS1 in the hash unit 2 shown in the far left side of Fig. 4A. It should be noted that, the authenticator CS1 is computed through the same sequence as that from ①' to ⑤' of the left portion in Fig. 3B, therefore, intermediate data generated in other hash unit 2 is not used.

The central portion in Fig. 4B shows a sequence of computing the authenticator CS2 in the hash unit 2 second from the left side in Fig. 4A. Herein, the authenticator CS2 is computed by using an intermediate result (L12) shown by arrow ⑥ obtained in the previous stage as the initial value through the same sequence as that from ①' to ⑤' shown in the left portion of Fig. 3B. Namely, in this second hash unit 2, the intermediate

data obtained in the first hash unit 2 is used.

The left portion of Fig. 4B shows a sequence of computing the authenticator CS3 in the hash unit 2 third from the left side in Fig. 4A. Herein, the authenticator CS3 is computed by using an intermediate result (L22) shown by arrow ⑦ obtained in the previous stage as the initial value through the same sequence as that from ①' to ⑤' shown in the left portion of Fig. 3B. Namely, in this third hash unit 2, the intermediate data obtained in the second hash unit 2 is used.

Through the above mentioned sequence, the hash units 2 are configured so as not to independently compute the authenticators CS1 to CS3 but to compute them in association with each other. This configuration allows a sequence of creation of the authenticators CS1 to CS3 to become more complicated, therefore, it becomes more difficult for a third party to forge the text data.

Fig. 6A and Fig. 6B are conceptual views for explaining safety of the authentication system used in this embodiment. Fig. 6A shows the concept of the present invention while Fig. 6B shows the concept of the conventional technology.

In Fig. 6B, a text space M is a virtual space possibly occupied by the text as an object to be forged, and the authenticator space is a virtual space possibly occupied by the authenticator. When the text space M corresponds to the authenticator space one to one, it becomes necessary to increase

the block length of the authenticator in order to make smaller a forged text space M_2 on the text space M in the manner shown with the circle indicated by a dotted line to the circle indicated by a solid line, so that a probability that the forged authenticator is by mistake recognized as the genuine authenticator is reduced.

However, as the block length of the authenticator depends on the processing block length of a hash function, the block length of the authenticator cannot be easily made longer.

Therefore, in the present invention, as shown in Fig. 6A, a forged space is made smaller by making use of a plurality of keys, so that the probability that the forged authenticator is by mistake recognized as the genuine authenticator is reduced. More specifically, assuming in Fig. 6A that a forged-text space on the text space M when the key K_1 is used is M_1 , that a forged text space on the text space M when the key K_2 is used is M_2 , and that a forged text space on the text space M when the key K_3 is used is M_3 , and when the keys K_1 , K_2 , and K_3 according to the present invention are used, the space for forgery is a space for forgery M_{123} which is extremely small and it is the area commonly shared by the spaces for forgery M_1 , M_2 , and M_3 , thus a probability that the data can be forged becomes still smaller.

As described above, in the present invention, the signing station creates a plurality of authenticators using a plurality

of one-way functions then and links these plurality of authenticators to the electronic data, while the certifying station compares the authenticators created from the electronic data which is separated from the received data with the authenticators included in this received data, and verifies whether the electronic data is a forged one or not. Therefore, with the present invention, even when the electronic data is a forged one, the probability of misidentification that the forged data may be erroneously recognized as an authentic data can greatly and easily be reduced, further, the probability of misidentification can be reduced through parallel processing without increasing the time required for preparing authenticators.

Furthermore, as the authenticator is truncated using a truncator, the probability of misidentification of a forged authenticator can further be reduced without increasing the amount of data required for the authenticator to be appended to the electronic data. In addition, intermediate data obtained when the authenticator is created in a previous stage is used as the initial value in the next stage, which allows the probability of misidentification to further be reduced.

The above description assumes that the object for processing is text data in a document. However, the present invention is not limited to the above case, but is also applicable to various types of multimedia data such as image

data, video data, or audio data. In addition, although it has been described above that a hash function is used as a one-way function, the present invention is not limited to the above case, and any one-way function other than the hash function may be used.

Although the invention has been described with respect to a specific embodiment for a complete and clear disclosure, the appended claims are not to be thus limited but are to be construed as embodying all modifications and alternative constructions that may occur to one skilled in the art which fairly fall within the basic teaching herein set forth.

WHAT IS CLAIMED IS:

1. An authentication system comprising:

a signing station which creates an authenticator by applying a one-way function to an information and then appends
5 a signature generated from the authenticator to the information;

a certifying station for checking the authentication of the information from the authenticator included in the data received from said signing station;

10 wherein said signing station has,

a first authenticator creating unit for dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

15 a linking unit for linking the plurality of authenticators created in said first authenticator creating unit to the information;

and said certifying station has,

a separating unit for separating the information and the
20 plurality of authenticators from the data received from said signing station;

a second authenticator creating unit for dividing the information separated by said separating unit into a plurality of data each having a prespecified length, and creating a
25 plurality of authenticators by applying a different one-way

function to each of the data; and

a certifying unit for comparing the plurality of authenticators created by said second authenticator creating unit with the plurality of authenticators separated from the information by said separating unit, and checking the authentication of the information.

2. An authentication system according to Claim 1; wherein said linking unit links the authenticators obtained by truncating the authenticators created by said first authenticator creating unit to the information, and

said certifying unit compares the authenticators obtained by truncating the authenticators created by said second authenticator creating unit to the authenticators separated from the information by said separating unit and checking the authentication of the information. .

3. An authentication system according to Claim 2; wherein said first authenticator creating unit and said second authenticator creating unit create a first authenticator by subjecting a first data to a one-way operation using a first key, and prepare a second authenticator by subjecting a second data to a one-way operation using a second key.

4. An authentication system according to Claim 3; wherein each of said first authenticator creating unit and said second authenticator creating unit discretely and independently creates the first authenticator and the second authenticator in parallel with each other.

5. An authentication system according to Claim 3; wherein each of said first authenticator creating unit and said second authenticator creating unit utilize an intermediate data when creating the second authenticator, which intermediate data is generated when the first authenticator is created.

6. An authentication method applied in an authentication system, wherein said authentication system has a signing station which creates an authenticator by applying a one-way function to an information and then appends a signature generated from the authenticator to the information, and a certifying station for checking the authentication of the information from the authenticator included in the data received from said signing station; wherein

said signing station executes,

a first authenticator creating step of dividing the information into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a transmitting step of linking the plurality of authenticators created in said first authenticator creating step to the information and transmitting the information to the certifying station; and

5 said certifying station executes,

a separating step of separating the information and the plurality of authenticators from the data received from said signing station;

10 a second authenticator creating step of dividing the information separated in said separating step into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

15 a certifying step of comparing the plurality of authenticators created in said second authenticator creating step with the plurality of authenticators separated from the information in said separating step, and checking the authentication of the information.

20 7. An authentication method according to Claim 6; wherein said transmitting step comprises a step of linking the authenticators obtained by truncating the authenticators created in said first authenticator creating step to the information, and

 said certifying step comprises a step of comparing the

authenticator obtained by truncating the authenticators created in said second authenticator creating step to the authenticators separated from the information in said separating step and a step of checking the authentication of the information.

8. An authentication method according to Claim 7; wherein said first authenticator creating step and said second authenticator creating step comprise a step of creating a first authenticator by subjecting a first data to a one-way operation using a first key, and a step of creating a second authenticator by subjecting a second data to a one-way operation using a second key.

9. An authentication method according to Claim 8; wherein each of said first authenticator creating step and said second authenticator creating step comprise a step of discretely and independently creating the first authenticator and the second authenticator in parallel with each other.

10. An authentication system according to Claim 8; wherein each of said first authenticator creating step and said second authenticator creating step comprise a step of utilizing an intermediate data when creating the second authenticator, which intermediate data is generated when the first authenticator is

created.

11. A computer-readable recording medium with a program
recorded therein for making a computer execute the
5 authentication method applied in an authentication system,
wherein said authentication system has a signing station which
creates an authenticator by applying a one-way function to an
information and then appends a signature generated from the
authenticator to the information, and a certifying station for
10 checking the authentication of the information from the
authenticator included in the data received from said signing
station; wherein

the program makes said signing station execute,

a first authenticator creating step of dividing the
15 information into a plurality of data each having a prespecified
length, and creating a plurality of authenticators by applying
a different one-way function to each of the data; and

a transmitting step of linking the plurality of
authenticators created in said first authenticator creating
20 step to the information and transmitting the information to the
certifying station; and

the program makes said certifying station execute,

a separating step of separating the information and the
plurality of authenticators from the data received from said
25 signing station;

a second authenticator creating step of dividing the information separated in said separating step into a plurality of data each having a prespecified length, and creating a plurality of authenticators by applying a different one-way function to each of the data; and

a certifying step of comparing the plurality of authenticators created in said second authenticator creating step with the plurality of authenticators separated from the information in said separating step, and checking the authentication of the information.

12. A signing apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information; said apparatus comprising:

a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a linking unit for linking the plurality of created authenticators to the information.

13. A signing apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information; said apparatus comprising:

5 a dividing unit for dividing the information into a plurality of data;

an authenticator creating unit for repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied.

10 a linking unit for linking the plurality of created authenticators to the information.

15 14. A certifying apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information as well as checks the authentication of the information; said apparatus comprising:

a separating unit for separating information and the plurality of authenticators from the data;

a dividing unit for dividing the information into a plurality of data;

25 an authenticator creating unit for creating an

authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a certifying unit for checking the authentication of the information based on each of the created authenticators and each
5 of the separated authenticators.

15. A certifying apparatus which creates an authenticator by utilizing a key and applying a one-way function to an information and then appends a signature to the information as
10 well as checks the authentication of the information; said apparatus comprising:

a separating unit for separating information and the plurality of authenticators from the data;

a dividing unit for dividing the information into a
15 plurality of data;

an authenticator creating unit for repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function
20 to a desired intermediate data the next data when the one-way function was applied; and

a certifying unit for checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

16. A computer-readable recording medium with a program recorded therein for making a computer execute:

a dividing step of dividing an information into a plurality of data;

5 an authenticator creating step of creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

a linking step of linking the plurality of created authenticators to the information.

10 17. A computer-readable recording medium with a program recorded therein for making a computer execute:

a dividing step of dividing an information into a plurality of data;

15 an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way
20 function was applied; and

a linking step of linking the plurality of created authenticators to the information.

18. A computer-readable recording medium with a program recorded therein for making a computer execute:

a separating step of separating information and a plurality of authenticators from the data;

5 a dividing step of dividing the information into a plurality of data;

an authenticator creating step of creating an authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and

10 a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

19. A computer-readable recording medium with a program recorded therein for making a computer execute:

a separating step of separating information and plurality of authenticators from a data;

a dividing step of dividing the information into a plurality of data;

20 an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way
25 function was applied; and

a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

- 5 20. A signing method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information; said method comprising:

10 a dividing step of dividing an information into a plurality of data;

an authenticator creating step of creating an authenticator by utilizing a key and applying a one-way function corresponding to each of the divided data; and

15 a linking step of linking the plurality of created authenticators to the information.

21. A signing method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information; said method comprising:

a dividing step of dividing an information into a plurality of data;

an authenticator creating step of repeating the creation of an authenticator by utilizing a key and applying a one-way function to one of the divided data as well as creation of an

25

authenticator by utilizing a key and applying a one-way function to a desired intermediate data the next data when the one-way function was applied; and

5 a linking step of linking the plurality of created authenticators to the information.

22. A certifying method in which an authenticator is created by utilizing a key and applying a one-way function to an information and then a signature is appended to the information
10 as well as the authentication of the information is checked; said method comprising:

a separating step of separating information and a plurality of authenticators from the data;

15 a dividing step of dividing the information into a plurality of data;

an authenticator creating step of creating an authenticators by utilizing a key and applying a one-way function corresponding to each of the divided data; and

20 a certifying step of checking the authentication of the information based on each of the created authenticators and each of the separated authenticators.

23. A certifying method in which an authenticator is created by utilizing a key and applying a one-way function to an
25 information and then a signature is appended to the information

as well as the authentication of the information is checked;
said method comprising:

a separating step of separating information and plurality
of authenticators from a data;

5 a dividing step of dividing the information into a
plurality of data;

an authenticator creating step of repeating the creation
of an authenticator by utilizing a key and applying a one-way
function to one of the divided data as well as creation of an
10 authenticator by utilizing a key and applying a one-way function
to a desired intermediate data the next data when the one-way
function was applied; and

a certifying step of checking the authentication of the
information based on each of the created authenticators and each
15 of the separated authenticators.

ABSTRACT OF THE DISCLOSURE

The authentication system has a signing station and a certifying station. The signing station divides the data to be transmitted into a plurality of data, a hash unit creates a plurality of authenticators by applying a different one-way function to each of the data. In the certifying station, a separating unit divides the data into a plurality of data, a hash unit creates a plurality of authenticators by applying a different one-way function to each data, and a comparing unit compares the authenticators prepared anew with the authenticators separated from the received data and checks the authentication of the data from the comparison.

FIG.1

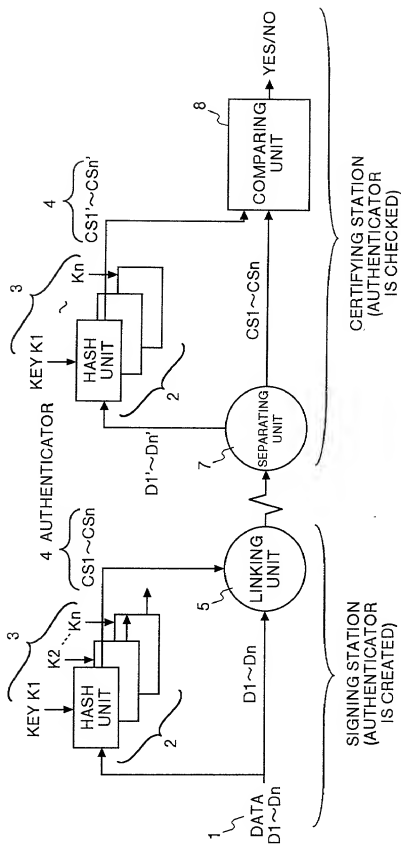


FIG.2A

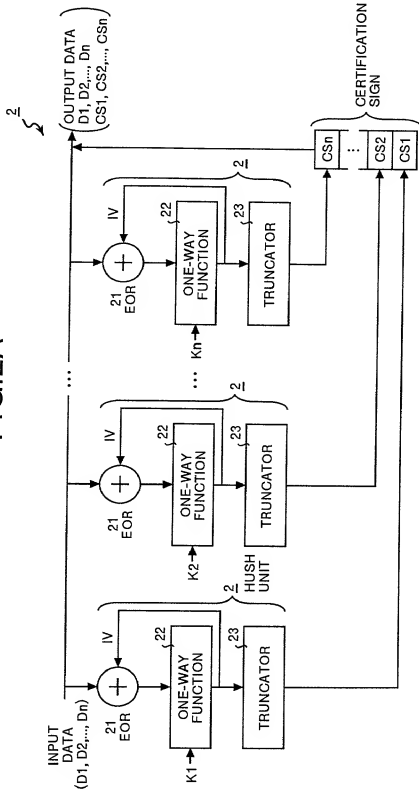


FIG.2B

- (b-1)CS1-GENERATING PROCESS
- ① → IV = PUBLIC CONSTANT
 - ② → EK1[IV(+D1)] = L11
 - ③ → EK1[L11(+D2)] = L12
 -
 - ④ → EK1[L1(n-1)(+Dn)] = L1n
 - ⑤ → Tr[L1n] = CS1
- (b-2)CS2-GENERATING PROCESS
- IV = PUBLIC CONSTANT
- EK2[IV(+D1)] = L21
- EK2[L21(+D2)] = L22
-
- EK2[L2(n-1)(+Dn)] = L2n
- Tr[L2n] = CS2
- (b-3)CS3-GENERATING PROCESS
- IV = PUBLIC CONSTANT
- EK3[IV(+D1)] = L31
- EK3[L31(+D2)] = L32
-
- EK3[L3(n-1)(+Dn)] = L3n
- Tr[L3n] = CS3

FIG.3A

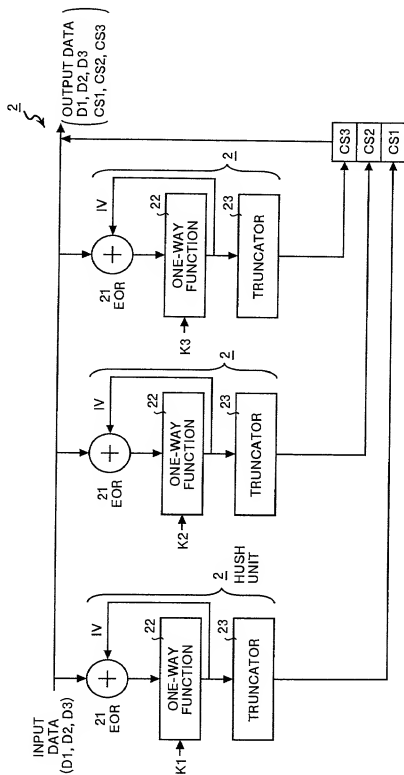


FIG.3B

- (b-1)CS1-GENERATING PROCESS
- ① $D1 \rightarrow IV \rightarrow \text{PUBLIC CONSTANT}$
 - ② $\rightarrow EK1[IV \oplus D1] = L11$
 - ③ $\rightarrow EK1[L11 \oplus D2] = L12$
 - ④ $\rightarrow EK1[L12 \oplus D3] = L13$
 - ⑤ $\rightarrow Tr[L13] = CS1$
- (b-2)CS2-GENERATING PROCESS
- IV = PUBLIC CONSTANT
- EK2[IV \oplus D1] = L21
 - EK2[L21 \oplus D2] = L22
 - EK2[L22 \oplus D3] = L23
 - Tr[L23] = CS2
- (b-3)CS3-GENERATING PROCESS
- IV = PUBLIC CONSTANT
- EK3[IV \oplus D1] = L31
 - EK3[L31 \oplus D2] = L32
 - EK3[L32 \oplus D3] = L33
 - Tr[L33] = CS3

FIG.4A

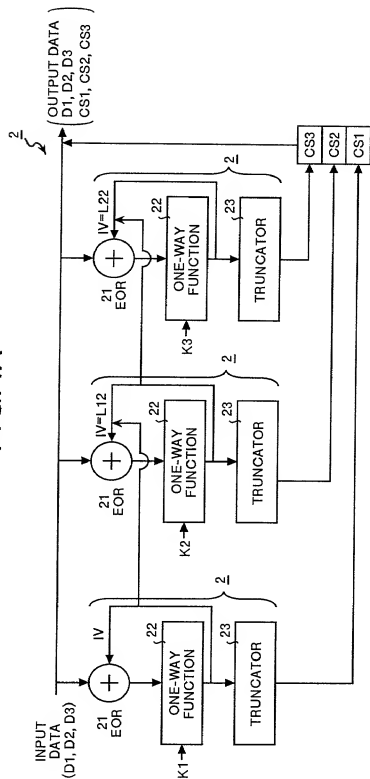


FIG.4B

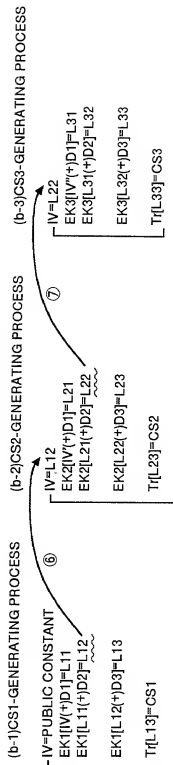


FIG.5

EXAMPLE OF A DOCUMENT

THE PRESENT INVENTION	
D ₁	D ₂
. 350Km/h	
• THE PRICE IS SET TO ONE MILLION.	
ABC AUTOMOBILE INDUSTRY AFE16085	

EXAMPLE OF A
AUTHENTICATOR IN A
DES-MAC SYSTEM
8 DIGITS (1 DIGIT=4 BITS)

FIG.6A

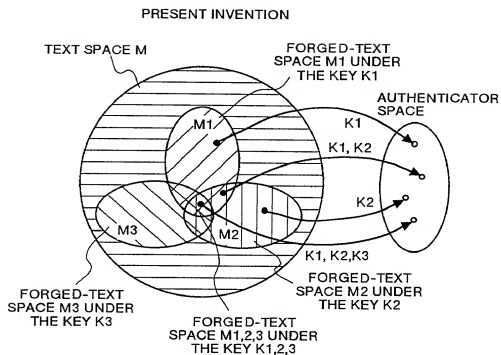
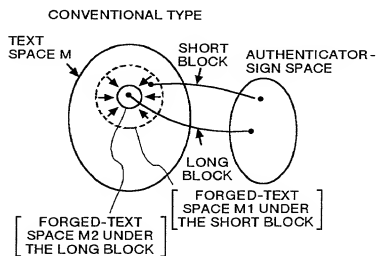


FIG.6B



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Declaration and Power of Attorney For Patent Application

特許出願宣言書及び委任状

Japanese Language Declaration

日本語宣言書

下々の氏名の発明者として、私は以下の通り宣言します。

As a below named inventor, I hereby declare that:

私の住所、私書箱、国籍は下記の私の氏名の後に記載された通りです。

My residence, post office address and citizenship are as stated next to my name.

下記の名称の発明に関して請求範囲に記載され、特許出願している発明内容について、私が最初かつ唯一の発明者（下記の氏名が一つの場合）もしくは最初かつ共同発明者であると（下記の名称が複数の場合）信じています。

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

AUTHENTICATION SYSTEM, AUTHENTICATION
METHOD, SIGNING APPARATUS, SIGNING
METHOD, CERTIFYING APPARATUS, CERTIFYING
METHOD, AND A COMPUTER-READABLE
RECORDING MEDIUM WITH A PROGRAM MAKING
A COMPUTER EXECUTE THE METHOD RECORDED
THEREIN

上記発明の明細書（下記の欄でx印がついていない場合は、本表に添付）は、

the specification of which is attached hereto unless the following box is checked:

☐ 月 日に出発され、米国出願番号または特許協定条約
国際出願番号を _____ とし、
（該当する場合） _____ に訂正されました。

☐ was filed on _____
as United States Application Number or
PCT International Application Number
_____ and was amended on
_____ (if applicable).

私は、特許請求範囲を含む上記訂正後の明細書を検討し、
内容を理解していることをここに表明します。

I hereby state that I have reviewed and understand the contents of
the above identified specification, including the claims, as
amended by any amendment referred to above.

私は、連邦規則法典第37編第1条56項に定規されると
おり、特許資格の有無について重要な情報を開示する義務が
あることを認めます。

I acknowledge the duty to disclose information which is material to
patentability as defined in Title 37, Code of Federal Regulations,
Section 1.56.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Japanese Language Declaration (日本語宣言書)

私は、米国法典第35編119条(a)-(d)項又は365条(b)項に基き下記の、米国外の国の少くとも一カ国を指定している特許協力条約365(a)項に基き国際出願、又は外国での特許出願もしくは発明者証の出願についての外国優先権をここに主張するとともに、優先権を主張している、本出願の前に出願された特許または発明者証の外国出願を以下に、枠内をマークすることで、示しています。

Prior Foreign Application(s)

外国での先行出願
11-88233

(Number)
(番号)

Japan

(Country)
(国名)

30/Mar./1999

(Day/Month/Year Filed)
(出願年月日)

Priority Not Claimed

優先権主張なし

☐

(Number)
(番号)

(Country)
(国名)

(Day/Month/Year Filed)
(出願年月日)

☐

私、第35編米国法典119条(e)項に基いて下記の米国外特許出願規定に記載された権利をここに主張いたします。

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Application No.)
(出願番号)

(Filing Date)
(出願日)

私は、下記の米国法典第35編120条に基いて下記の米国外特許出願に記載された権利、又は米国外を指定している特許協力条約365条(c)に基き権利をここに主張します。また、本出願の各請求範囲の内容が米国法典第35編112条第1項又は特許協力条約で規定された方法で先行する米国外特許出願に開示されていない限り、その先行米国外特許提出日以後で本出願の日本国内または特許協力条約国際提出日までの期間中に入手された、連邦規則法典第37編1.56項で定義された特許資格の有無に関する重要な情報について開示漏れがあることを認識しています。

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Status: Patented, Pending, Abandoned)
(現況: 特許許可済、係属中、放棄済)

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Status: Patented, Pending, Abandoned)
(現況: 特許許可済、係属中、放棄済)

私は、私自身の知識に基いて本宣言書中で私が行なう表明が真実であり、かつ私の入手した情報と私の信じていること、さらに故意に基き虚偽の表明及びそれと同等の行為は米国法典第18編1001条に基き、罰金または拘禁、もしくはその両方により処罰されること、そしてそのような故意による虚偽の表明を行なえば、出願した、又は既に許可された特許の有効性が失われることを認識し、よってここに上記のごとく宣誓を致します。

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below.

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s), or 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of application.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Japanese Language Declaration
(日本語宣言書)委任状: 私は下記の発明者として、本出願に関する一切の
手続を米特許商標局に対して遂行する弁護士または代理人
として、下記の者を指名いたします。(弁護士、または代理
人の氏名及び登録番号を明記のこと)James D. Halsey, Jr., 22,729; Harry John Stass, 22,010; David M. Picher, 25,908; John C. Garvey, 28,607; J. Randall Beckers,
30,358; William F. Herbert, 31,024; Richard A. Gollhofer, 31,106; Mark J. Henry, 36,162; Gene M. Garner II, 34,172; Michael D.
Stein, 37,240; Paul I. Kravetz, 35,230; Gerald P. Joyce, III, 37,648; Todd E. Mariette, 35,269; Harlan B. Williams, Jr., 34,756;
George N. Stevens, 36,938; Michael C. Soldner, 41,455; Norman L. Ourada, 41,235; Kevin R. Spivak, P-43,148; and William M.
Scherrier, 35,348 (agent)

書類送付先

POWER OF ATTORNEY: As a named inventor, I hereby appoint
the following attorney(s) and/or agent(s) to prosecute this
application and transact all business in the Patent and Trademark
Office connected therewith (list name and registration number)

Send Correspondence to:

STAAS & HALSEY
700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001

直接電話連絡先: (名前及び電話番号)

Direct Telephone Calls to: (name and telephone number)

STAAS & HALSEY
(202) 434-1500

唯一または第一発明者名	Full name of sole or first inventor	
	Ryota AKIYAMA	
発明者の署名	Inventor's signature	Date
日付	<i>Ryota Akiyama</i>	Sep. 22, 1999
住所	Residence	
	Kanagawa, Japan	
国籍	Citizenship	
	Japanese	
私書箱	Post Office Address	
	c/o FUJITSU LIMITED	
	1-1, Kamikodanaka 4-chome,	
	Nakahara-ku, Kawasaki-shi,	
	Kanagawa 211-8588 Japan	
第二共同発明者	Full name of second joint inventor, if any	
	Seigo KOTANI	
第二共同発明者	Second joint inventor's signature	Date
日付	<i>Seigo Kotani</i>	Sep. 22, 1999
住所	Residence	
	Kanagawa, Japan	
国籍	Citizenship	
	Japanese	
私書箱	Post Office Address	
	c/o FUJITSU LIMITED	
	1-1, Kamikodanaka 4-chome,	
	Nakahara-ku, Kawasaki-shi,	
	Kanagawa 211-8588 Japan	

(第三以降の共同発明者についても同様に記載し、署名を
すること)(Supply similar information and signature for third and subsequent
joint inventors.)

第三共同発明者		Full name of third joint inventor, if any Takayuki HASEBE
第三共同発明者	日付	Third inventor's signature Date <i>Takayuki Hasebe</i> Sep. 22, 1999
住 所		Residence Kanagawa, Japan
国 籍		Citizenship Japanese
私書箱		Post Office Address c/o FUJITSU LIMITED 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan
第四共同発明者		Full name of fourth joint inventor, if any Takaoki SASAKI
第四共同発明者	日付	Fourth inventor's signature Date <i>Takaoki Sasaki</i> Sep. 22, 1999
住 所		Residence Tokyo, Japan
国 籍		Citizenship Japanese
私書箱		Post Office Address c/o Fujitsu Basic Software Corporation 15-33, Shibaura 4-chome, Minato-ku, Tokyo 108-8531 Japan

第五共同発明者		Full name of fifth joint inventor, if any
第五共同発明者	日付	Fifth inventor's signature Date
住 所		Residence
国 籍		Citizenship
私書箱		Post Office Address
第六共同発明者		Full name of sixth joint inventor, if any
第六共同発明者	日付	Sixth inventor's signature Date
住 所		Residence
国 籍		Citizenship
私書箱		Post Office Address

(第七以降の共同発明者についても同様に
記載し、署名をすること)

(Supply similar information and signature for
seventh and subsequent joint inventors.)